

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Records and Information associated the cellular telephone  
assigned IP Address 2607:fb90:e103:6511:9426:aa55: 7dc7:  
f730 at 2021-06-08 21:18:27 UTC, more fully described in  
Attachment A

Case No. 21-881M(NJ)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure  
of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before June 24, 2021 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

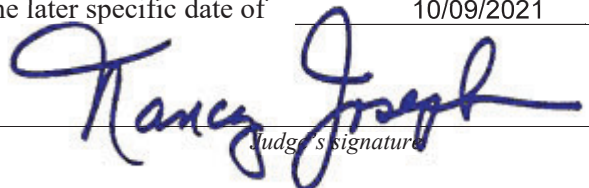
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Nancy Joseph

(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 10/09/2021

Date and time issued: June 10, 2021 @ 5:15p.m.City and state: Milwaukee, WI


Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return					
Case No.:		Date and time warrant executed:		Copy of warrant and inventory left with:	
Inventory made in the presence of :					
Inventory of the property taken and name(s) of any person(s) seized:             					
Certification					
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____ _____ <i>Executing officer's signature</i> _____ <i>Printed name and title</i></p>					

## **ATTACHMENT A**

### **Property to Be Searched**

1. Records and information associated with the cellular device assigned IP Address **2607:fb90:e103:6511:9426:aa55:7dc7:f730** at **2021-06-08 21:18:27 UTC** (referred to herein and in Attachment B as “the Target Cell Phone”), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the “Service Provider”), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany NJ, 07054.
2. The Target Cell Phone.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of May 15, 2021, to the date of this warrant's execution:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:
  - (A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - (ii) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received) as well as per-call measurement data (also known as “real-time tool” or “RTT”).
- b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:
  - i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
  - ii. Source and destination telephone numbers;
  - iii. Date, time, and duration of communication; and
  - iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as “real-time tool” or “RTT”).
- c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. “Information about the location of the Target Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.
  - i. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

- ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities relating to a violation of 18 U.S.C. §1073 involving KEVION MINOR, since April 30, 2021.

All information described above in Section I that will assist in arresting KEVION MINOR, who was charged on May 20, 2021, with violating 18 U.S.C. §1073, and who is the subject of an arrest warrant issued on May 20, 2021, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

## In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*Records and Information associated the cellular telephone  
assigned IP Address 2607:fb90:e103:6511:9426:aa55:7dc7:f730  
at 2021-06-08 21:18:27 UTC, more fully described in Attachment A

Case No. 21-881M(NJ)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

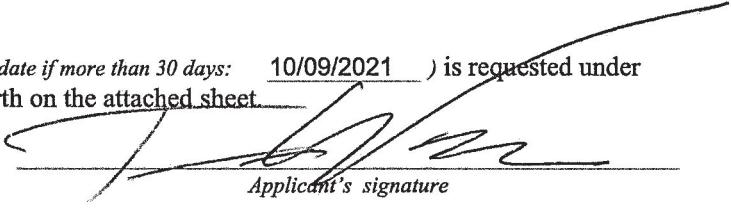
The search is related to a violation of:

Code Section  
18 U.S.C. § 1073Offense Description  
Unlawful flight to avoid prosecution

The application is based on these facts:

See affidavit

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 90 days *(give exact ending date if more than 30 days: 10/09/2021)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Timothy Walther, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone \_\_\_\_\_ *(specify reliable electronic means)*.Date: June 10, 2021City and state: Milwaukee, WI  
Judge's signature

Nancy Joseph

Printed name and title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Timothy J. Walther, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A), for information about the location of the cellular telephone assigned **IP Address 2607:fb90:e103:6511:9426:aa55:7dc7:f730 at 2021-06-08 21:18:27 UTC** (the “**Target Cell Phone**”), whose service provider is T-Mobile (“Service Provider”), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany NJ, 07054. The **Target Cell Phone** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

3. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been employed as such since March 2008. Since November 2019, I have been assigned to the Milwaukee FBI Violent Crimes Task Force. My current responsibilities include investigating violations of federal law related to violent crimes including homicide, non-fatal shootings, firearm violations, armed bank robbery, armed commercial robberies, and other related federal offenses defined under Title 18 of the United States Code.

4. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

5. The facts in this affidavit come from my training and experience, my review of documents, and information obtained from other agents/law enforcement officers. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that KEVION MINOR has violated 18 U.S.C. § 1073 (Unlawful flight to avoid prosecution). As such, on May 20, 2021, a criminal complaint and associated arrest warrant was filed in the Eastern District of Wisconsin for a violation of 18 U.S.C. § 1073. There is also probable cause to believe that the information described in Attachment B will assist law enforcement in locating and arresting MINOR, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

7. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined 18 U.S.C. Section 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. Section 2711(3)(A)(i).

#### **PROBABLE CAUSE**

8. On May 6, 2021, the Racine County District Attorney’s Office filed an eight-count criminal complaint against KEVION A. MINOR under case number 2021CF000760. The complaint charges MINOR with the following:

- a. Two Counts of Attempted First Degree Intentional Homicide, contrary to Wis. Stat. 940.01(1)(a), 939.50(3)(a), 939.32, 939.62(1)(c), 939.63(1)(b), and 973.055(1). This charge is a Class B felony punishable by up to 60 years of imprisonment, subject to

penalty enhancers;

- b. Three Counts of First Degree Recklessly Endangering Safety, contrary to Wis. Stat. 941.30(1), 939.50(3)(f), 939.6195(2), 939.62(1)(c), and 939.63(1)(b). This charge is a Class F felony punishable by up to 12 years and 6 months of imprisonment, subject to penalty enhancers;
- c. One Count of Stalking, contrary to Wis. Stat. 940.32(3)(c), 939.50(3)(f), 939.6195(2), 939.62(1)(c), and 939.055(1). This charge is a Class F felony punishable by up to 12 years and 6 months of imprisonment, subject to penalty enhancers;
- d. One Count of Possession of a Firearm by a Felon, contrary to Wis. Stat. 941.29(1m)(a), 939.50(3)(g), 939.6195(2), and 939.62(1)(b). This charge is a Class G felony punishable by up to 10 years in prison, subject to penalty enhancers; and
- e. One Count of Armed Burglary, contrary to Wis. Stat. 943.10(2)(a), 939.50(3)(e), 939.6195(2), and 939.62(1)(c). This charge is a Class E felony punishable by up to 15 years of imprisonment, subject to penalty enhancers.

9. An arrest warrant issued on May 6, 2021.

10. The criminal complaint alleges that on April 30, 2021, at approximately 5:45 p.m., the Racine Police Department was dispatched to a person shot at a residence in the 3300 block of Hamlin Street, Racine, Wisconsin. Upon arrival, officers identified a single gunshot victim who was identified as Victim #1. Victim #1 had suffered gunshot wounds to the leg and abdomen.

11. Subsequent investigation and interviews identified the shooter as KEVION A. MINOR. MINOR is the father of a minor child who resides at the above residence with her mother, Victim #2. Victim #2 told officers that before the shooting, she was sitting in her residence when she observed MINOR exit a gold colored sedan and approach the residence with a pistol in his hand. Victim #2 stated that MINOR has been threatening her recently and believed he was there to kill her.

12. Victim #2 stated that she immediately ran to the back bedroom in an attempt to hide and was joined by her step-father, Victim #1. As they attempted to secure the door, MINOR forced his arm through the door opening while holding the pistol. As MINOR was attempting to gain access to the bedroom he stated, “you bitch ass nigga, you trying to block me from [Victim #2]; I’ll kill you.”

13. As MINOR pointed the pistol at Victim #1 through the door opening, Victim #1 grabbed the gun and struggled with MINOR over possession of the pistol. It was during this struggle Victim #1 was shot twice.

14. Immediately after the shooting, MINOR fled the residence and to date has not been taken into custody.

15. Before the shooting, MINOR threatened Victim #2 and her family through video messages. One of MINOR's threats to Victim #2 was as follows: ". . . I'm telling you right now it's on with everybody, it's on. I don't give a fuck about none ya'll bitch, I don't care about me, I don't care about my daughter being around me bitch, I'm killing every last one of ya'll until they catch me, and when they catch me. . ."

16. Since the shooting, law enforcement has made numerous attempts to locate and arrest MINOR. On May 3, 2021, a warrant to locate/track MINOR's cellular telephone was authorized by the Racine County Circuit Court. On May 6, 2021, MINOR was tracked to a Lake County, Illinois hotel, but he was able to evade capture. Law enforcement subsequently located MINOR in Waukegan, Illinois, at two local business establishments, but again were unsuccessful in taking MINOR into custody.

17. At present, MINOR has discontinued use of the this previously identified telephone number.

18. Law enforcement has identified MINOR's Facebook Account. Specifically, members of the Racine Police Department located and reviewed the publicly accessible Facebook page for [www.facebook.com/Kt.duce.5](https://www.facebook.com/Kt.duce.5) and observed photos of the account user posted to the account. These photos were subsequently compared to historical Racine County Jail booking photos of MINOR, and it was determined to be the same person. Therefore, law enforcement believes that MINOR uses and/or controls the Facebook Account [www.facebook.com/Kt.duce.5](https://www.facebook.com/Kt.duce.5).

19. On May 4, 2021, a pen register / trap and trace order was authorized by the Racine County Circuit Court for this Facebook Account ([www.facebook.com/Kt.duce.5](http://www.facebook.com/Kt.duce.5)).

20. Results of the on-going pen register / trap and trace on the above referenced Facebook account show that between the issuance of the order on May 4, 2021, and June 8, 2021, IP addresses associated with account activity have a significant number of the IP address log-ins associated with T-Mobile. The most recent log-in was with **IP Address 2607:fb90:e103:6511:9426:aa55:7dc7:f730**, the **Target Cell Phone**, on June 8, 2021, at approximately 21:18:27 UTC Time.

21. Law enforcement believes that the location information associated with the most recent Facebook account log-in will reveal the most current whereabouts of MINOR.

#### **TECHNICAL BACKGROUND: DYNAMIC IP ADDRESSES**

22. Your affiant used the website [www.arin.net](http://www.arin.net), the “American Registry of Internet Numbers (ARIN),” to obtain the owner and operator of the IP address mentioned previously: **2607:fb90:e103:6511:9426:aa55:7dc7:f730**. According to ARIN, the listed IP address is owned and operated by T-Mobile. Your affiant has used ARIN in the past and knows this website to be reliable.

23. Based on training and experience, I know that T-Mobile is a cellular service provider and does have the ability to connect their cellular service to the internet through Dynamic Internet Protocols. A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it’s connected to a network. A dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node.

24. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP

addresses, dynamic IP addresses are not permanent. A dynamic IP is assigned to a node until it's connected to the network; therefore, the same node may have a different IP address every time it reconnects with the network.

25. I know through training and experience that T-Mobile is able to “resolve” associated Dynamic IP addresses. When T-Mobile “resolves” those IP addresses, they are able to identify the associated user and the specific cellular phone associated with that user. In other words, when T-Mobile is provided with a particular associated IP address and time stamp (like the IP address and time stamp described here), T-Mobile is able to (i) determine the particular cellular phone that used that IP address; and (ii) collect cell-site location data associated with that same particular cellular phone, in the manner described below.

#### **TECHNICAL BACKGROUND: CELL SITE LOCATION DATA**

26. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

27. Based on my training and experience, I know that the Service Provider can

collect cell-site data on a prospective basis about the **Target Cell Phone**. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

28. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data. Based on my training and experience, I know that the Service Provider can collect E-911 Phase II data about the location of the **Target Cell Phone**, including by initiating a signal to determine the location of the **Target Cell Phone** on the Service Provider's network or with such other reference points as may be reasonably available.

29. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication’s content.

30. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers’ use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the **Target Cell Phone**’s user or users and may assist in the identification of co-conspirators and/or victims.

31. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

32. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

33. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the **Target Cell Phone** on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

34. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 90 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the **Target Cell Phone** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

35. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **Target Cell Phone** outside of daytime hours.

## **ATTACHMENT A**

### **Property to Be Searched**

1. Records and information associated with the cellular device assigned IP Address **2607:fb90:e103:6511:9426:aa55:7dc7:f730** at **2021-06-08 21:18:27 UTC** (referred to herein and in Attachment B as “the Target Cell Phone”), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the “Service Provider”), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany NJ, 07054.
2. The Target Cell Phone.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of May 15, 2021, to the date of this warrant's execution:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:
  - (A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - (ii) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received) as well as per-call measurement data (also known as “real-time tool” or “RTT”).
- b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:
  - i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
  - ii. Source and destination telephone numbers;
  - iii. Date, time, and duration of communication; and
  - iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as “real-time tool” or “RTT”).
- c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. “Information about the location of the Target Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.
  - i. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

- ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities relating to a violation of 18 U.S.C. §1073 involving KEVION MINOR, since April 30, 2021.

All information described above in Section I that will assist in arresting KEVION MINOR, who was charged on May 20, 2021, with violating 18 U.S.C. §1073, and who is the subject of an arrest warrant issued on May 20, 2021, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.